# 不定方程式の可解性と代数多様体の有理点について(代数的数論 : 最近の進展とその背景)

AUTHOR(S):

森田, 康夫

CITATION:

森田, 康夫. 不定方程式の可解性と代数多様体の有理点について(代数的数論 : 最近の進展とその背景). 数理解析研究所講究録 1993, 844: 1-16

ISSUE DATE:

1993-06

URL:

http://hdl.handle.net/2433/83608

数理解析研究所講究録
第844巻 1993年 1-16



# 不定方程式の可解性と代数多様体の有理点について

森田 康夫 (東北大学・理学部)

## §0 序.

代数多様体上の有理点の分布を調べる事を主な研究テーマとする場合、そのような有理点の分布を有限回の操作で完全に決定する事が最終目標となる。しかし、不定方程式の可解性に関する Hilbert の第10問題の否定的解決により、一般にはこのような事は不可能である。

これに対し1次元の代数曲線の場合には、G. Faltings 等の研究により、このような事が出来るものと考えられている。

このような見地より、著者は、『有理点の分布を完全には決定出来ない代数曲面が見つかるのではないか？』と言う予想 (期待) を持って、代数曲面上の有理点の分布を詳しく調べている。

本文の前半では、Hilbert の第10問題がどのように解決されたかを、M. Davis の論文 [D] をもとに解説し、(i) 整数論を研究する人間にとってどのような問題が残されているかをコメントし、また (ii) 代数多様体の上の有理点を研究する立場から、この事がどのようなことを意味するかについてコメントする。

また後半では、代数体上の有理点の分布に関し、Batyrev と Manin により作られた予想 ([B-M] 参照) に基づき、現在どのような事が解っていたり、予想されたりしているかを、代数曲面の場合の著者の仕事を中心にして解説する。

## §1. Hilbert の第10問題.

### 1-1. 問題.

Hilbert は1900年にパリで開かれた国際数学者会議で、20世紀のうちに研究されるべき問題を23あげたが、そのうちの第10問題として、不定方程式の可解性に関する次の問題がある：

**Hilbert's $10^{\text{th}}$ problem:**

Find an algorithm to test Diophantine equations for solvability in $\mathbb{Z}$.

この問題は、当然肯定的に解かれるべき問題として出題されたようだが、その後、この問題の中に出て来る『アルゴリズム』と言うものが何で有るべきかを研究するうち、この問題を肯定的に解く事が出来ない事が解った ([D-M-R] 等参照)。

以下 [D] にしたがって、その事を紹介する。

**1-2. 問題の簡易化.**

次のような事を考える：

整数係数の多項式 $P_i(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ と整数 $x_1,\ldots,x_n \in \mathbb{Z}$ について、

$$P_1(x_1,\ldots,x_n) = 0,\ P_2(x_1,\ldots,x_n) = 0,\ \ldots,\ P_m(x_1,\ldots,x_n) = 0$$

$$\Longleftrightarrow \quad (P_1^2 + P_2^2 + \ldots + P_m^2)(x_1,\ldots,x_n) = 0$$

つまり、『連立の不定方程式 $P_i(x_1,\ldots,x_n) = 0\ (\forall i = 1,\ldots,m)$ を解く事は、単独の不定方程式 $(P_1^2 + P_2^2 + \ldots + P_m^2)(x_1,\ldots,x_n) = 0$ を解く事と同値である。』同様にして、次の事も解る。

$$P_1(x_1,\ldots,x_n) = 0,\ \ or\ \ P_2(x_1,\ldots,x_n) = 0,\ \ \ldots,\ \ or\ \ P_m(x_1,\ldots,x_n) = 0$$

$$\Longleftrightarrow \quad (P_1 \cdot P_2 \cdot \ldots \cdot P_m)(x_1,\ldots,x_n) = 0$$

さて、任意の自然数は、四つの整数の2乗の和の形に書ける。したがって、$P(x) \in \mathbb{Z}[x]$ とするとき、

$$P(x) = 0\ (\exists x \in \mathbb{Z}) \Longleftrightarrow P(x) \cdot P(0) \cdot P(-x) = 0\ (\exists x \in \mathrm{N})$$

$$P(x) = 0\ (\exists x \in \mathrm{N}) \Longleftrightarrow P(1 + y_1^2 + y_2^2 + y_3^2 + y_4^2) = 0\ (\exists y_i \in \mathbb{Z})$$

がなりたつ。したがって、変数の数を増やし同様の事をすると、『整数の範囲で任意の不定方程式が解を持つかどうかを判定する事と、自然数の範囲で任意の不定方程式が解を持つかどうかを判定する事とは同値である。』ことが解る。

Hilbert の第10問題では、整数環 $\mathbb{Z}$ における連立の不定方程式の解の存在、非存在の判定を問題とするが、以上のような事に注意すると、次の問題を調べれば十分である事が解る：

『単独の不定方程式

$$P(x_1,\ldots,x_n) = 0$$

の、自然数の範囲における解 $x_1,\ldots,x_n \in \mathrm{N}$ が存在するかどうかを判定せよ。』

**1-3. 帰納的関数.**

自然数の組 $\mathrm{N}^m$ の上で定義され、自然数 N に値を取る関数に対し、帰納的関数と言う概念を以下のようしてに定める。これは、アルゴリズムと言う言葉を精密化しようと言う研究の結果、見つかった概念である。

**定義 R.** 次の 初期関数 $c(x),\ s(x),\ U^i(x_1,\ldots,x_n)$ より始め、(1) 合成、(2) 帰納法、(3) 最小化 の3つの手続きを繰り返して作られる関数を**帰納的関数**と呼ぶ：

$$c(x) = 1,\ \ s(x) = x + 1,\ \ U_i^n(x_1,\ldots,x_n) = x_i\ (1 \leq i \leq n)$$

(1) **合成**. 与えられた関数 $g_i(x_1,\ldots,x_m)$ $(1 \leq i \leq m)$, $f(x_1,\ldots,x_m)$ より、次のようにして合成関数 $h$ を作る：

$$h(x_1,\ldots,x_n) := f(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)).$$

(2) **帰納法**. 与えられた関数 $f$, $g$ より次のようにして、帰納的に新しい関数 $h$ を作る：

$$h(x_1,\ldots,x_n,1) := f(x_1,\ldots,x_n)$$

$$h(x_1,\ldots,x_n,t+1) := g(t,h(x_1,\ldots,x_n,t),x_1,\ldots,x_n).$$

(3) **最小化**. 関数 $f$, $g$ で、任意の $x_1,\ldots,x_n \in \mathrm{N}$ に対し、$f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n,y)$ を満たす $y \in \mathrm{N}$ が少なくとも 1 つ存在するものが与えられたとする。この時、このような $y \in \mathrm{N}$ のうちで最小の $y$ を使って、新しい関数 $h$ を定義する：

$$h(x_1,\ldots,x_n) := \min_y[f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n,y).]$$

このように定義された帰納的関数の概念は、A. Church 、 K. Gödel 、S. C. Kleene 、A. M. Turing 、E. L. Post 等の人により、$\lambda$–定義可能な関数の概念や Turing Machine の概念と同値である事が解った。そこで A. Church は、値を計算するアルゴリズムを持つ関数とは、実は帰納的関数の事を指すのだと言う事を提案した：

**Church の仮説**. 値を計算するアルゴリズムを持つ関数と言うのは、上で定めた帰納的関数の事を言う。

この仮説は、上で述べた 3 つの概念の同値性と、現実にこれ以外に値が計算できる関数が見つかっていないと言う事実を根拠として、 正しいものと考えられている ([Hi] 等参照)。

**1-4. 不定方程式型の関数.**

$\mathrm{N}^n$ の部分集合や、$\mathrm{N}^n$ の上の関数に対し、不定方程式型という概念を次のようにして定義する。

これは、不定方程式の可解性と非常に密接に結び付いた概念であり、これが **1-4** において定義された帰納的関数の概念と一致する事を証明することにより、Hilbert の第 10 問題は否定的に解決された。

**定義 D**. $S \subset \mathrm{N}^n$ が **不定方程式型** であるとは、適当な多項式 $P(x_1,\ldots,x_n,y_1,\ldots,y_m) \in \mathbb{Z}[x_1,\ldots,x_n,y_1,\ldots,y_m]$ で、次の同値条件を満たすものが存在する事を言う：

任意の $(x_1,\ldots,x_n) \in \mathbb{Z}^n$ にたいし、

$$(x_1,\ldots,x_n) \in S \iff P(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0 \quad (\exists y_1,\ldots,y_m \in \mathrm{N}).$$

関数 $f:\mathrm{N}^n \longrightarrow \mathrm{N}$ が **不定方程式型**であるとは、そのグラフが不定方程式型である事を言う。

明らかに、$f:\mathrm{N}^n \longrightarrow \mathrm{N}$ が、整数係数の多項式で与えられる関数なら、不定方程式型の関数である。しかし、それ以外にも不定方程式型の関数は沢山存在する。

**命題**. 次の性質 (1), (2) を満たす不定方程式型の関数 $P(x,y),\ L(z), R(z)$ が存在する：
(1) $L(P(x,y)) = x,\ R(P(x,y)) = y\ (\forall x,y \in \mathrm{N})$.
(2) $P(L(z),R(z)) = z,\ L(z) \leq z,\ R(z) \leq z\ (\forall z \in \mathrm{N})$.

(注意). この命題の $P(x,y):\mathrm{N}^2 \longrightarrow \mathrm{N}$ は 1 対 1, onto であり、$(L,R):\mathrm{N} \longrightarrow \mathrm{N}^2$ は $P(x,y)$ の逆写像を与える。

命題の証明. $T(n) := n(n+1)/2$ と置く。$T(n)$ は単調増加関数であるから、任意の自然数 $z$ に対し、非負整数 $n$ で、

$$T(n) < z \leq T(n+1) = T(n)+(n+1)$$

を満たすものが唯一つ存在する。したがって、任意の $z \in \mathrm{N}$ は、適当な $n \leq 0$ と $y \in \mathrm{N}$ を使い、$z = T(n)+y,\ y \leq n+1$ と一意的に表現出来る。言い直すと、任意の $z \in \mathrm{N}$ は、適当な $x,\ y \in \mathrm{N}$ を使い

$$z = T(x+y-2)+y$$

と一意的に表す事が出来る。そこで $x = L(z),\ y = R(z)$ と置く。また

$$P(x,y) := T(x+y-2)+y-1$$

により関数 $P(x,y)$ を定義する。

$$z = P(x,y) \iff 2z = (x+y-2)(x+y-1)+2y$$
$$x = L(z) \iff (\exists y)\ [2z = (x+y-2)(x+y-1)+2y]$$
$$y = R(z) \iff (\exists x)\ [2z = (x+y-2)(x+y-1)+2y]$$

を満たすから、これらは不定方程式型の関数であり、定義より求める性質を持つ事が解る。

(注意). 次のようにして定義される関数 $S(i,u):\mathrm{N}^2 \longrightarrow \mathrm{N}$ も不定方程式型である：
$w \equiv L(u) \bmod (1+iR(u)),\ w \leq 1+iR(u)$ を満たす $\exists! w \in \mathrm{N}$ を取り、$S(i,w) := w$ と定める。

さて Hilbert の第 10 問題に関する M. Davis, J. Robinson, Y. Matijasevich らによる数学基礎論的研究の主結果は、次の定理である：

**定理 M**. 関数 $f:\mathrm{N}^n \longrightarrow \mathrm{N}$ は、不定方程式型の関数であるとき、その時に限り、帰納的関数となる。

不定方程式型の関数が帰納的関数である事は、容易に証明出来る。
逆に帰納的関数が不定方程式型であるだろうと言う事は、Davis 等により研究され、ごく初期より予想されていたようであるが、Robinson は、指数関数

$$n^x:\mathrm{N} \ni x \longmapsto n^x \in \mathrm{N}\ (n \in \mathrm{N})$$

が不定方程式型である事を証明すれば良い事を示した。そこで Matijasevich は、Fibonacci 数

$$a_1 = a_2 = 1, \quad a_{n+1} = a_n + a_{n-1}$$

が $n$ が増加する時、$a_n$ も指数関数的に増加する事を示す事により、この事を証明し、Davis, Robinson の結果と合わせ、上記の定理 M の証明を完結し、Hilbert の第 10 問題を否定的に解決した。

なおこの証明の途中で得られた次の結果は、定理 M の証明の本質的な部分を占める：

『整数係数の多項式 $P(t, z, x_1, \ldots, x_n, y_1, \ldots, y_m)$ が与えられたとき、

$\{(t, x_1, \ldots, x_n) \in \mathrm{N}^{n+1} \mid (\forall z \leq t)(\exists y_1, \ldots, y_m)$ such that $P(t, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$

と言う集合は不定方程式型である。』

**1-5. 反例の構成.**

これまでの結果を使って、Hilbert の第 10 問題が解けない例を具体的に構成する。

$x_0, x_1, x_2, x_3, \ldots$ を無限個の変数とし、$R(z)$, $L(z)$ を **1-4** において構成した不定方程式型の関数とし、多項式 $\{P_i \mid i \in \mathrm{N}\} \subset \mathrm{N}[x_0, x_1, x_2, x_3, \ldots]$ を帰納的に構成する：

$$P_1 := 1$$
$$P_{3i-1} := x_{i-1}$$
$$P_{3i} := P_{L(i)} + P_{R(i)}$$
$$P_{3i+1} := P_{L(i)} \cdot P_{R(i)}$$

$\{(L(i), R(i)) \mid i \in \mathrm{N}\} = \mathrm{N} \times \mathrm{N}$ であるから、$\{P_i \mid i \in \mathrm{N}\}$ は全ての $\mathrm{N}[x_0, x_1, x_2, x_3, \ldots]$ の多項式を表す。したがって、N の任意の不定方程式型の部分集合は、或る $n \in \mathrm{N}$ を使い

$$D_n := \{ x_0 \in \mathrm{N} \mid (\exists x_1, \cdots, x_n) \text{ such that } P_{L(n)}(x_0, x_1, \cdots, x_n) = P_{R(n)}(x_0, x_1, \cdots, x_n) \}$$

の形に書ける。さらに次の定理が成り立つ。

**定理.** $\{ (n, x) \in \mathrm{N}^2 \mid x \in D_n \}$ は不定方程式型の集合である。

**略証.** $x \in D_n \iff (\exists u) \{S(1, u) = 1 \;\&\; S(2, u) = x$
$\;\&\; (\forall i)_{i \leq n} [S(3i, u) = S(L(i), u) + S(R(i), u)]$
$\;\&\; (\forall i)_{i \leq n} [S(3i+1, u) = S(L(i), u) \cdot S(R(i), u)]$
$\;\&\; S(L(n), u) = S(R(n), u)\}$

に注意する。これは **1-4** の最後に書いた事より、不定方程式型の集合になる。

$$V := \{ n \in \mathrm{N} \mid n \notin D_n \}.$$

と置き、Cantor の対角線論法を使うと、次の定理が得られる。

**定理.** $V$ は不定方程式型の集合ではない。

証明. $D_1$, $D_2$, $D_3$,... は全ての不定方程式型の集合をつくす。したがって、もし $V$ が不定方程式型なら、ある $i \in \mathrm{N}$ を取ると $V = D_i$ が成り立つ。よって、

$$i \in D_i \iff i \in V \iff i \notin D_i$$

となり、矛盾が生じる。

$$\chi(z) = \begin{cases} 1 & z \in V \text{ のとき} \\ 0 & \text{その他のとき} \end{cases}$$

により $V$ の定義関数 $\chi(z)$ を定義する。定理 M と Church の仮説により、

不定方程式型の関数 $\iff$ 帰納的関数 $\iff$ 値を計算するアルゴリズムを持つ関数

が成り立つ。したがって、

**系.** $\chi(z)$ の値を計算するアルゴリズムは存在しない。

不定方程式型の集合 $\{ (n,x) \in \mathrm{N}^2 \mid x \in D_n \}$ を定める不定方程式を $P(n, x, z_1, \ldots, z_k) = 0$ とする。このとき、

$$n \in D_n \iff (\exists z_1, \ldots, z_k \in \mathrm{N}) \text{ such that } P(n, n, z_1, \ldots, z_k) = 0$$

が成り立つ。よって、任意の $n \in \mathrm{N}$ に対し、

$$P(n, n, z_1, \ldots, z_k) = 0$$

が自然数解を持つかどうかを判定するアルゴリズムは存在しない。したがって、

**定理 H_10** . Hilbert の第 10 問題の解を与えるアルゴリズムは、存在しない。

**1-6. 残された問題等.**

以上では、$\mathbb{Z}$ 係数の不定方程式の $\mathbb{Z}$ または N における解を扱った。しかし、整数論的立場からは、

$(I_k)$ 有限次代数体 $k$ の整数環 $I_k$ において同様の問題を研究する事や、

$(\mathbb{Q})$ $\mathbb{Q}$ や有限次代数体 $k$ 上で同様の問題を研究する事

が必要となる。

問題 $(I_k)$ については、J. Denef が研究し、$I_k$ が 2 次体の整数環の場合に $\mathbb{Z}$ の場合と同様の結果を得ている。

この問題は、適当な $I_k$ 係数の多項式、$P(t, x_1, \ldots, x_n)$ で

$$\{t \in I_k \mid P(t, x_1, \ldots, x_n) = 0 \ (\text{ for some } \exists x_1, \ldots, x_n \in I_k)\} = \mathbb{Z}$$

なるものが見つかれば、$I_k$ 上でも $\mathbb{Z}$ と同様の結果が得られる ([D-M-R] 等参照) 。この問題を解く事は、簡単ではないようだが、本質的な困難は存在しないように思う。

問題 $(\mathbb{Q})$ については、かなり本質的な困難さが有るように思う。
しかし、$\mathbb{Q}$ の上で全ての解を求める事が出来れば、$\mathbb{Z}$ での解も全て求まり、Hilbert の第 10 問題が肯定的に解ける。これは **1-5** の結果に反するから、『$\mathbb{Q}$ の上で全ての解を求める事は出来ない。』ことは解る。

さて問題 $(\mathbb{Q})$ を解くには、$\mathbb{Z}$ の場合の結果に帰着する方法と、$\mathbb{Q}$ や $k$ 上で理論を作り直す方法が考えられる。

$\mathbb{Q}$ の場合に分母を払い、$\mathbb{Z}$ の場合に帰着しようとすると、自明な解の存在が扱いを面倒にする。

$\mathbb{Q}$ 上で $\mathbb{Z}$ と同様の事を行おうとすると、『どのようにして不定方程式型の集合や関数を定義するか？』がまず問題になる。

$S \subset \mathbb{Q}^n$ が不定方程式型である事を、適当な多項式 $P \in \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ で、次の同値条件を満たすものが存在する場合に言う事にする：

任意の $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ にたいし、

$$(x_1, \ldots, x_n) \in S \iff P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \quad (\exists y_1, \ldots, y_m \in \mathbb{Q}).$$

与えられた有理数に対し、その分子および分母は明らかに計算できるが、任意の有理数に対しその分子を計算する関数を、(上の意味で) 不定方程式型の関数として構成するのは困難に見える。
しかし、このようにして定義される不定方程式型の関数の概念が、どのような関数を含むかを研究する事は、かなり意味のある事と思われる。

これについてのもう一つのアイデアは、$S \subset \mathbb{Q}^n$ が不定方程式型である事を、適当な多項式 $P \in \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ で、次の同値条件を満たすものが存在する場合に言う事にするものである：

任意の $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ にたいし、

$$(x_1, \ldots, x_n) \in S \iff P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \quad (\exists y_1, \ldots, y_m \in \mathrm{N}).$$

このようにすると、分子を計算する関数は不定方程式型になる。しかし、『$\mathbb{Q}$ に係数をもつ多項式の N の範囲での解を考える。』と言う不自然さは、深刻な問題を引き起こす可能性が有る。

## §2. 代数多様体の上の有理点の分布、Batyrev-Manin の予想等.

### 2-1. 小平次元による代数多様体の分類.

$V$ をコンパクトな複素多様体とし、$K = K_V$ を $V$ の canonical line bundle とする。このとき、canonical ring $R(U)$ を使って、$V$ の**小平次元** $\kappa(V)$ を次のように定義する ([B-P-V], [U] 等参照)。

$$R(V) := \mathbb{C} \oplus \sum_{m \geq 1} \Gamma(V, K_V^{\otimes m})$$

$$\kappa(V) := \begin{cases} -\infty & \cdots \quad R(V) = \mathbb{C} \text{ のとき} \\ \mathrm{trdeg}\,(R(V)) - 1 & \cdots \quad \text{その他} \end{cases}$$

定義より、小平次元は

$$\kappa(V) = -\infty,\ 0,\ 1,\ \ldots,\ \dim(V)$$

となる。

小平次元の意味を説明するため、$\dim(V) = 1$ とする。したがって、$V$ は非特異な**代数曲線**であるとし、$g(V)$ をその種数 (genus) とする。この場合、Riemann-Roch の定理により

$$\begin{aligned} \kappa(V) = -\infty &\iff g(V) = 0 \\ \kappa(V) = 0 &\iff g(V) = 1 \\ \kappa(V) = 1 &\iff g(V) \geq 2 \end{aligned}$$

となる。代数曲線の性質を研究する場合には、種数が 0 のとき、1 のとき、$\geq 2$ のときに応じて $V$ の性質は異なるが、その理由が小平次元の違いとして説明される。

次に、著者が現在最も興味を持っている、$V$ が完備かつ非特異な**代数曲面**である場合を取り上げる。したがって、$\dim(V) = 2$ で、しかも $V$ は代数多様体であるとする。さらに $V$ は第 1 種の例外曲面を持たず、したがって**極小** (relatively minimal) であるとする。

このとき、Enriques 等により、次の分類が得られている ([B-P-V] 等参照):

$\kappa(V) = -\infty \iff V$ は射影空間 $\mathbb{P}^2(\mathbb{C})$ または 線織面 (a ruled surface)

$\kappa(V) = 0 \iff V$ はアーベル曲面, 超楕円曲面 (a hyper-elliptic surface), K3-曲面, または Enriques 曲面

$\kappa(V) = 1 \iff V$ は proper な楕円曲面 (a proper elliptic surface)

$\kappa(V) = 2 \iff V$ は一般型 (general type) の代数曲面

(注意) 1. 線織面とは代数曲線の上の $\mathbb{P}^1$−bundle を言う。
2. 超楕円曲面はアーベル曲面を、Enriques 曲面は K3-曲面を、不分岐被覆として持つ。
3. proper elliptic surface は 楕円曲面であるから、一般ファイバーが楕円曲線である、代数曲線上のファイバー空間である。

**2-2. Batyrev-Manin の予想.**

$k$ を有限次代数体 ( $[k:\mathbb{Q}] < \infty$ ) とし、$V$ を $k$ 上定義された射影多様体、$K = K_V$ を $V$ の canonical line bundle 、$L$ を $V$ 上の ample line bundle とする。

$NS(V)$ を $V$ の Néron Severi group とする。$NS(V)$ は $V \times_k \overline{k}$ の divisor group を代数的同値と言う関係で割ったものであり、有限生成アーベル群となる ([Ful], p.385 等参照)。$N^1(V) := NS(V) \otimes_{\mathbb{Z}} \mathbb{R}$ とおく。これは有限次元ベクトル空間となる。

$N^1(V)$ の中で $\overline{k}$−rational で effective な divisors の全体が生成する closed subcone を $N^1_{\text{eff}} = N^1_{\text{eff}}(V)$ で表し、

$$\alpha(L) := \inf \{ \gamma \in \mathbb{R} \mid \gamma [L] + K_V \in N^1_{\text{eff}} \} \in \mathbb{R}$$

で **幾何学的不変量** $\alpha(L)$ を定義する。

$L$ は ample な line bundle であるから、それを使って absolute height

$$H_L : V(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$$

が定義できる。$H_L$ は $k$ の取り方には依らないが、$L$ から作られる $V$ の射影空間への埋め込みに依るため、modulo bounded functions でしか定まらない。

$U$ を $V$ の $k$−open subset とし、次のようにしてゼータ関数 $Z_U(L;s)$ を定義する：

$$Z_U(L;s) := \sum_{x \in U(k)} h_L(x)^{-s}$$

この級数は $\mathrm{Re}(s)$ が十分大きいとき収束する事が解るので、$Z_U(L;s)$ が収束する $\sigma = \mathrm{Re}(s)$ の inf として、**整数論的不変量** $\beta_U(L)$ を定義する：

$$\beta_U(L) := \inf \{ \sigma \in \mathbb{R} \mid Z_U(L,s) \text{ は } \mathrm{Re}(s) = \sigma \text{ で収束する} \} \in \mathbb{R}_{\geq 0} \cup \{-\infty\}$$

これは、$H_L$ を modulo bounded functions での類から選ぶ選び方には依らず、$U$ と $L$ により一意的に定まる。

V. V. Batyrev と Yu. I. Manin は、以上のように定義した 2 つの不変量の間に次の関係が成り立つ事を予想した ([B-M] 参照)：

**予想** (Batyrev-Manin). 任意の $\varepsilon > 0$ に対し、$V$ の ( Zariski 位相に関する) ある open dense な部分集合 $U = U(L,\varepsilon)$ で次の不等号を満たすものが存在する：

$$\beta_U(L) \leq \alpha(L) + \varepsilon$$

(注意). [B-M] では $\alpha(L)$ を定義するときに使う $N^1_{\text{eff}}$ 等が、$V$ のものか、$V \times_k \overline{k}$ のものかがはっきりしない。しかし、これらについて次の事が解る：

(1) $k-$上定義された divisor が、$\overline{k}-$に移って algebraically equivalent to 0 となるなら、$k-$上では torsion divisor であり ([Ful], p.185, Proposition 10.3 参照)、$N^1(V) := NS(V) \otimes_{\mathbb{Z}} \mathbb{R}$ の中では 0 となる。よって、$NS(V)$ を $k-$rational な divisors を $k-$上 algebraically equivalent to 0 なもので割ったものと定義しても、以下の議論に影響は及ぼさない。

(2) $N^1_{k,\mathrm{eff}}$ を $NS(V)$ の中で $k-$rational かつ effective な divisors の全体の生成する closed cone とし、それより $\alpha(L)$ と同様にして $\alpha(k,L)$ を定義する。このとき、$k$ が大きくなると、$N^1_{k,\mathrm{eff}}$ は大きくなり、したがって $\alpha(k,L)$ は単調減少する。さらに $k$ が $\overline{k}$ に近づくとき、$\alpha(k,L)$ は $\alpha(L)$ に近づく。他方 $k$ が大きくなると、$U(k)$ の点が増えるから、$Z_U(L;s)$ の収束性が悪くなり、$\beta_U(L)$ は単調増加する。この事より、『全ての $k$ に対し $\alpha(L)$ を$\alpha(k,L)$ で置き換えた形の予想が成り立つなら、$\alpha(L)$ に対する上の形の予想が成り立つ』事が解る。逆に『上の形の予想が成り立つなら、$\alpha(L)$ を $\alpha(k,L)$ で置き換えた予想が成り立つ』のは明らかである。

**2-3. 代数曲線の場合の結果.**

$V = C$ を完備非特異な代数曲線とする。$C$ 上の line bundle を $L$ とすると、

$L$ : ample $\iff \deg(L) > 0$

が成立ち、

$\{L \mid C$上の line bundle$\} \ni L \longmapsto \deg(L) \in \mathbb{Z}$

なる対応により、$NS(C) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}$ が成り立つ。

$\deg(K_C) = 2g(C) - 2$

であるから、容易な計算により

$\alpha(L) = -(2g(C) - 2)/\deg(L)$

となる事が解る。

そこで小平次元 $\kappa(C)$ の価に応じて、Batyrev-Manin の予想などがどうなるかを調べて見る。

[$g = 0$]. $\kappa(C) = -\infty \iff g(C) = 0$

であるとする。このとき、$L$ が ample なら上記の計算より $\alpha(L) > 0$ となる。

一般に『$C$ は 2 次曲線と $k$ 上で同型である。』ことが、Riemann-Roch の定理から証明できるが、『もし $C(k) \neq \emptyset$ なら、$C(k) \cong \mathbb{P}^1(k)$ が成り立つ。』ことも解る。したがってこの場合には、$C$ 上の有理点の分布が解るから、$Z_U(L,s)$ が計算でき、

$$\beta_C(L) = -(2g(C) - 2)/\deg(L) = \alpha(L)$$

が成り立つ事が証明出来る。

[$g = 1$]. $\kappa(C) = 0 \iff g(C) = 1$

だとする。このとき、$K \cong \mathcal{O}_C$ となり、$L$ を任意の ample line bundle とするとき、$\alpha(L) = 0$ が成り立つ。

もし $C(k) \neq \emptyset$ であるなら、$C$ は $k$ 上定義された楕円曲線 (アーベル多様体) の構造を持つ。さらに『$k$ が素体上有限生成な体なら、$C(k)$ は有限生成アーベル群となる。』(L. J. Mordell による結果、後に A. Weil により一般のアーベル多様体の場合に拡張された。) したがって、$C(k)$ の torsion points は有限群であり、$C(k) \otimes_{\mathbb{Z}} \mathbb{R}$ は有限次元の $\mathbb{R}-$ベクトル空間となる。

A. Néron と J. Tate は、アーベル多様体の上の height functions の性質を調べ、canonical height $h_L(x)$ と言う性質の良い関数を構成した。これは absolute height $H_L(x)$ との間に、

$h_L(x) = \log H_L(x) + O(1)$

なる関係を満たす $C(\overline{\mathbb{Q}})$ 上の関数であり、$L$ が symmetric なら、$h_L$ は torsion points の上では 0 となり、ベクトル空間 $C(k)\otimes_{\mathbb{Z}}\mathbb{R}$ の上の正定値な二次形式を与える。

『正定値な二次形式を持つ $n$ 次元のベクトル空間において、半径 $r$ の超球の中入る格子点の数は、$O(r^n)$ 』である。これを使うと $C$ 上の $k$−有理点の数が上から評価でき、

$$\beta_C(L) = 0 = \alpha(L)$$

が成り立つ事が解る。

$[g \geq 2]$. $\kappa(C) = 1 \iff g(C) \geq 2$

であるとする。このとき任意の ample line bundle $L$ に対し、$\alpha(L) < 0$ が成り立つ。そこで $\varepsilon$ を十分小さく取り、 $\varepsilon + \alpha(L) < 0$ と成るようにする。このとき、Batyrev-Manin の予想を認めると、ある $C$ の $k$−open subset $U$ で、

$$\beta_U(L) < 0 \iff U(k) \text{ は有限集合}$$

となるものが存在する。したがって、$C \setminus U$ は有限集合であるから、$C(k)$ 自身有限集合となる。

この事は、『 $g(C) \geq 2$ の場合には、$C(k)$ は有限集合となる。』と言う Mordell により予想 (**Mordell conjecture**) され、G. Faltings により証明された結果を意味する。

(注意). 1 次元の代数曲線の場合には、$C(k)$ を有限回の計算で求める事が可能であろうと思われている。

$g(C) \geq 2$ の場合には、この事は **effective Mordell conjecture** と呼ばれ、G. Wüstoholtz 他の人により超越数論の方法 (Baker の方法) を使って研究されている。

$g(C) = 1$ の場合には、$C(k) \neq \emptyset$ の場合には、『 Tate-Shafarevich 群の位数が有限なら、有限生成アーベル群 $C(k)$ の生成元を見つける事が出来る。』しかし、『 $C(k)$ が空であるかどうかを有限回で判定するアルゴリズム』を、著者は知らない。

この場合、$C(k) \neq \emptyset$ かどうかを調べるときの障害は、$g(C) - 1 = 0$ であるため、canonical bundle から effective divisor が作れず、したがって Riemann-Roch の定理が使いにくい所にある。いずれにしろこの場合には、楕円曲線の Galois twist 等としての調べる事により、この問題を解決する事が可能ではないかと思われる。

**2-4. 代数曲面の場合など.**

$\kappa(V) = -\infty$ なる場合には、次の結果が知られている：

**定理** (Châtelet). $V$ が代数体 $k$ 上定義された代数多様体で、$V$ は $\overline{k}$ 上で $\mathbb{P}^n$ と同型となるものとする。このとき、もし $V(k) \neq \emptyset$ なら、$V$ は $k$ 上で $\mathbb{P}^n$ と同型である ([Ch] 参照)。

$A$ が $k$ 上定義された代数多様体で、$A \times_k \overline{\mathbb{Q}}$ が**アーベル多様体**となるものとする。この場合 canonical bundle $K_A$ は自明であり、したがって $\alpha(L) = 0$ となる。

もし $A(k) \neq \emptyset$ であれば、$A(k)$ は有限生成なアーベル群で、有限次元ベクトル空間 $A(k)\otimes_{\mathbb{Z}}\mathbb{R}$ の上には canonical height $h_L$ が存在する。したがって、**2-3** と同様にして $\beta_A(L) = 0$ となる。よって

$$\beta_A(L) = -\infty \text{ or } 0 \quad \leq \quad 0 = \alpha(L)$$

となり、$U = A$ として Batyrev-Manin の予想が成り立つ。

次に $\kappa(V) = \dim(V)$ が成り立つものとする。このとき、$V$ は**一般型** (general type) であると言う。

この場合には、小平邦彦 (と P. Vojta) により $\alpha(L) < 0$ が成り立つ事が知られている ([C-S], p.349, Lemma 4.1 参照)。よって $\varepsilon$ を十分小さく取ると、$\varepsilon + \alpha(L) < 0$ となる。したがって、Batyrev-Manin の予想を認めると、ある $V$ の $k$−open subset $U$ で、

$$\beta_U(L) < 0 \iff U(k) \text{ は有限集合}$$

となるものが存在する。この事は、E. Bombieri と P. Vojta により予想されていた事 **(Bombieri-Vojta 予想)** である。

(注意). この予想は、現在まだ証明されていないが、$V$ がアーベル多様体の部分多様体で、$\{0\}$ 以外のアーベル多様体を含まないなら、$V(k)$ 自身が有限集合となる事が G. Faltings により証明されている ([Sz] 等参照)。

$Y$ を $k$ 上定義された完備かつ非特異な代数多様体、$L$ を $Y$ 上の ample line bundle とし、$f : X \longrightarrow Y$ を $k$ の拡大体上で定義された不分岐被覆とする。$K$ を $k$ の有限次拡大体で、$X$, $f$ が定義されるものとする。

$f$ は不分岐被覆だから、$Y \times_k K$ の canonical bundle $K_Y \times_k K$ を $f$ により $X$ へ持ち上げた $f^*(K_Y \times_k K)$ は $X$ の canonical bundle $K_X$ と同型になり、$Y$ 上の ample line bundle $L$ を $X$ まで持ち上げた $f^*(L \times_k K)$ は $X$ 上の ample line bundle になる ([H], p. 232, Ex. **5.7**, (d) 参照)。

また $f^*$ は、algebraically equivalent to 0 な divisor を、algebraically equivalent to 0 な divisor に写す ([Ful], p.185, Proposition 10.3 参照 )。したがって、$f^*$ は $N^1(Y \times_k K)$ を $N^1(X)$ に写す。さらに $f^*$ が effective divisor を effective divisor に写す事は明らかである。したがって、$f^*$ は、$N^1_{\text{eff}}(Y \times_k K)$ を $N^1_{\text{eff}}(X)$ に写す。

よって、任意の $\gamma \in \mathbb{R}$ に対し

$$\gamma \cdot [L] + K_Y \in N^1_{\text{eff}}(Y) \quad \Longrightarrow \quad \gamma \cdot [f^*(L \times_k K)] + K_X \in N^1_{\text{eff}}(X)$$

が成り立つ。したがって、

$$\alpha(L) \geq \alpha(f^*(L \times_k K))$$

が成り立つ。( $N^1_{\text{eff}}$ を $\overline{k}$−上のものを使って定義した事から、実は等号が成り立つ。) $K$ を任意の $K$ の有限次拡大体 $M$ で置き換えても、この等式が成り立つ事に注意しておく。

$f : X \longrightarrow Y$ は不分岐被覆だから、$K$ の有限次拡大体 $M$ で、$f^{-1}(Y(K)) \subset X(M)$ となるものが存在する ([S], p.50, Chevalley-Weil Theorem 参照)。

そこで $X \times_k M$ とその上の ample な $f^*(L \times_k M)$ に対し Batyrev-Manin の予想が成り立つとすると、任意の $\varepsilon > 0$ に対し、或る $X \times_k M$ の $M$−open dense な部分集合 $V$ が存在し、

$$\beta_V(f^*(L \times_k M)) \leq \alpha(f^*(L \times_k M)) + \varepsilon$$

が成り立つ。ここで必要なら $V$ を $M/k$ 上の共役全体の共通部分で置き換える事により、$V$ は $k$ 上定義され、$V_0 \times_k M$ の形であるとして良い。

$f : X \longrightarrow Y$ は不分岐被覆だから、proper mapping であり、$f((X \times_k M) \setminus V) = f((X \setminus V_0) \times_k M) \subset Y \times_k M$ は $Y \times_k M$ の Zariski $k$−closed な部分集合である。そこで、

$$U := Y \setminus (f(X \setminus V_0))$$

と置く。これは $Y$ の $k$−open dense な部分集合である。

$H_{f^*(L \times_k K)} = \mathrm{O}(1) \times \{H_L \circ f\}$ であるから、任意の $\sigma > 0$ に対して

$$Z_U(L, \sigma) \leq \mathrm{O}(1)^{-\sigma} \times Z_{V_0 \times_k M}(f^*(L \times_k M), \sigma)$$

が成立つ。よって

$$\beta_U(L) \leq \beta_{V_0 \times_k M}(f^*(L \times_k M)) \leq \alpha(f^*(L \times_k M)) + \varepsilon \leq \alpha(L) + \varepsilon$$

が成り立つ。したがって、

**命題 U**. $f : X \longrightarrow Y$, $L$, $k$, $M$ 等を上のとうりとする。したがって、$X$ は $Y$ の不分岐被覆で、$M$ は $k$ の有限次拡大だとする。このとき、$X \times_k M$ と $f^*(L \times_k M)$ に対して Batyrev-Manin の予想が成り立つなら、$Y$ と $L$ に対しても Batyrev-Manin の予想が成り立つ。

以下 $S$ は (完備非特異かつ第 1 種の例外曲線を持たない) **代数曲面**であるとする。

$S$ の小平次元が $-\infty$ だとする。

もし、$S \times_k \overline{\mathbb{Q}} \cong \mathbb{P}^2$ の時は、前に書いた Châtelet の結果により、( $S \neq \emptyset$ と仮定すると) $S$ 上の有理点の分布は解る。

$S$ は $k$ 上定義された代数多様体で、$S \times_k \overline{\mathbb{Q}}$ が ruled surface $\overline{\pi} : \overline{S} \longrightarrow \overline{C}$ となるものとする。

ruled surfaces の代数的閉体上の分類とその自己同型群の構造は、丸山正樹等により研究されている ([H], [Ma] 等参照)。

$\overline{C}$ の種数が 2 以上だとする。この場合には、自己同型群に関する丸山の結果を使うと、適当な $k$ 上定義された代数曲線 $C$ が有り、$\overline{\pi} : \overline{S} \longrightarrow \overline{C}$ は $k$ 上定義された $\pi : S \longrightarrow C$ を $\overline{k}$ まで持ち上げた形になる事が証明できる。したがって、$S(k) \subset \pi^{-1}(C(k))$ となるから、有限集合 $C(k)$ 上の $\pi$ のファイバーを調べる事により、$S(k)$ の構造は解る。

$\overline{C}$ の種数が 0 だとすると、$\overline{S}$ は $\mathbb{P}^1 \times \mathbb{P}^1$ か、Hirzuburch 曲面 $\mathbb{P}(\mathcal{O} \oplus \mathcal{O}(n))$ となる。$\mathbb{P}^1 \times \mathbb{P}^1$ の場合には、次の定理が証明できる :

**定理**. $S$ が代数体 $k$ 上定義された代数曲面で、$S \times_k \overline{k} \cong \mathbb{P}^1 \times \mathbb{P}^1$ となるものとする。このとき、もし $S(k) \neq \emptyset$ なら、$S \cong \mathbb{P}^1 \times \mathbb{P}^1$ ($k$−同型) となるか、適当な 2 次拡大 $K/k$ が存在し、$S \cong \mathrm{R}_{K/k}(\mathbb{P}^1 \times_k K)$ ($k$−同型) となる。ここで $\mathrm{R}_{K/k}$ は $K$ 上の多様体から $k$ 上の多様体を作る Weil の functor である。

これ以外の Hirzeburch 曲面の場合には、$S$ が $k$−有理点を持つなら、$k$ 上で Hirzeburch 曲面 $\mathbb{P}(\mathcal{O} \oplus \mathcal{O}(n))$ と同型となる事が証明出来る。

$\overline{C}$ の種数が 1 の場合には、decomposable でない ruled surface が存在するため、種数が 0 の場合より調べるのが面倒になる。しかしその場合にも、ruled surfaces の分類と automorphism groups の決定がなされている。したがって、この場合にも種数が 0 の場合と大体同様の結果が得られる ([M2] 参照)。

$S$ がアーベル曲面の場合には、前に書いた様に、Batyrev-Manin の予想などが証明されている。

$S$ が**超楕円曲面**だとする。このとき、あるアーベル曲面 $A$ からの不分岐な被覆

$$f : A \longrightarrow S$$

が存在する。したがって、命題 U により、この場合にも Batyrev-Manin の予想が成り立つ ([M-S] 参照)。

一般に『アーベル多様体を不分岐な被覆として持つ任意の多様体に対し、Batyrev-Manin の予想は成り立つ。』

同様にして、$S$ を Enriques 曲面とすると、ある K3-曲面 $T$ と 2 次の不分岐被覆写像 $f : T \longrightarrow S$ が存在する。したがって、命題 U により、『K3-曲面 $T$ に対して Batyrev-Manin の予想が成り立つなら、Enriques 曲面 $S$ に対しても Batyrev-Manin の予想が成り立つ。』

$S$ を**一般型の代数曲面**とし、

$$\alpha : S \longrightarrow A$$

を Albanese mapping とする。これは $S$ からアーベル多様体への写像のうち、最も普遍的な写像である。

$\dim A = 0$ なら、これは何も情報を与えない。

$\dim \mathrm{Im}(\alpha) = 1$ だとする。このときには、$\alpha$ の像は非特異な代数曲線 $C$ で、しかも $\alpha$ は $S$ から $C$ の上へのファイバー空間の構造を与える。普遍性より、$C$ はアーベル多様体 $A$ を群として生成しているから、$g(C) = \dim A$ である。もしこれが 1 なら $C$ は無限個の有理点を持ち、余り多くの情報を与えないように思われる。しかし、これが 2 以上なら、Faltings の定理により、$C(k)$ は有限集合となり、$S(k)$ は有限個の $\alpha$ のファイバーに含まれる。したがってこの場合には、1 次元の場合に帰着される。

$\dim \mathrm{Im}(\alpha) \geq 2$ だとする。この場合 $\mathrm{Im}(\alpha)$ はアーベル多様体 $A$ の部分多様体で、$A$ を群として生成している。このようなものは、一般型の代数多様体の上のアーベル多様体をファイバーとしてもつファイバー空間の構造を持つ ([U] 参照)。したがって、$\mathrm{Im}(\alpha)$ は (i) アーベル曲面であるか、(ii) 種数 2 以上の代数曲線の上の楕円曲面の構造を持つか、(iii) アーベル多様体の $\kappa(V) = \dim(V)$ となる部分多様体となる。これら 3 つのうち第 2 のものの有理点の研究は、1 次元の場合に帰着する。第 3 のものは、前記の Faltings の研究 ([Sz] 参照) と密接に関係している。第 1 のものは、代数幾何的な研究が有る様だが、Faltings の方法がこの場合にも使えないかどうか、研究に値すると思う。

いずれにしても、一般型の代数曲面に対しては、どうなるべきかの予想が存在し、また完全ではないまでも有る程度の結果も証明出来る。

以上において $S$ は極小 (relatively minimal) であるとしてが、有理曲面 (rational surface) 以外の場合には、与えられた体上 $k$ 上で極小モデルが作れる。したがって、これらの場合には、極小だとの仮定は重要ではない。

結局問題として残ったのは、
(1) 有理曲面の場合の極小でない場合の扱い、
(2) K3-曲面の上の有理点の研究、および
(3) proper elliptic surface の上の有理点の研究
の 3 つである。

このうち (2) については、$S$ を楕円曲線のべき $E \times E$ を自己同型の群 $\{\pm\mathrm{id}\}$ で割って、それの特異点を解消した場合を考えれば解るように、$S$ の上には一般には有理曲線が $\infty$ 個のっている。そのため、それ以外の有理点を調べる事が非常に難しくなっている。この事がこの場合の問題の難しさの所在であると思われる。

(3) についても難しさは、(2) と似ている。この場合には、楕円曲面としての sections および multi-sections が無限個存在しうる。そのため、これらの上にない有理点の性質を調べるのが難しくなっている。

## References

[B-M] V. V. Batyrev et Yu. I. Manin, Sur le nombre des points rationnels de hauteur borné des varietés algèbriques, Math. Ann., **286**(1990), 27-43.

[B-P-V] W. Barth, C. Peters and Van de Ven, Compact complex surfaces, Erg. der Mat., 3. Folge, Band 4, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1984.

[Ch] F. Châtelet, Variations sur un thème de Poincaré, Ann. Sic. École Norm. Sup., **61**(1944), 249-300.

[C-S] G. Cornell and J. H. Silverman, Arithmetic Geometry, Springer-Verlag, New York Berlin Heidelberg London Paris Tokyo, 1985.

[D] M. Davis, Hilbert tenth problem is unsolvable, Amer. Math. Monthly, **80**(1973), 233-269.

[D-M-R] M. Davis, Y. Matijasevich and J. Robinson, Hilbert's tenth problem. Diophantine equations: Positive aspect of a negative solution, Proc. Symp. in Pure Math., **28**(1976), 323-378.

[F] G. Faltings, Endlichkeitssätze für Abelsche Varietäten über Zahl- körpern, Invent. Math., **73**(1983), 349-366.

[FGA] A. Grothendieck, Fondements de la Géométrie Algébrique, Secrétariat Math., Paris, 1962.

[Ful] W. Fulton, Intersection theory, Erg. der Mat., 3. Folge, Band 2, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1984.

[H] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York - Heidelberg - Berlin 1977.

[Hi] 廣瀬健, 帰納的関数, 共立出版, 1989.

[Ma] M. Maruyama, On classification of ruled surfaces, Lect. in Math., Dept. of Math., Kyoto Univ. **3**, Kinokuniya, Tokyo 1970.

[M1] 森田康夫, 代数曲面の有理点について, 第 35 回代数学シンポジウム報告集, 1989, 209-230.

[M2] Y. Morita, Forms of ruled surfaces defined over algebraic number fields which have at least one rational point, to appear

[M-S] Y. Morita and A. Sato, Distribution of rational points on hyperelliptic surfaces, Tohoku Math. J., **44**(1992), 345-358.

[S] J.-P. Serre, Lecture on the Mordell-Weil theorem, Vieweg, Braunsweg, 1989.

[Sz] L. Szpiro, Sur les solution d'un systèm d'équationa polynomiales sur une variété alélienne, Sém. Bourbaki, **42**(1989-90), $n°$ 729.

[U] K. Ueno, Classification theory of algebraic varieties and compact complex spaces, Lecture Notes in Math., **439**(1975).